日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　２月１９日

出願番号
Application Number: 特願２００３－０４１４８５

[ST. 10/C]: [ＪＰ２００３－０４１４８５]

出願人
Applicant(s): 株式会社東芝

２００３年　７月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５７５０６

【書類名】　特許願

【整理番号】　A000205440

【提出日】　平成15年 2月19日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 15/00

【発明の名称】　サーバ装置、鍵管理装置、暗号通信方法及びプログラム

【請求項の数】　23

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　金井　達徳

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　關　俊文

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　吉田　英樹

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　崎山　伸夫

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100108855

【弁理士】

【氏名又は名称】　蔵田　昌俊

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　サーバ装置、鍵管理装置、暗号通信方法及びプログラム

【特許請求の範囲】

【請求項１】

クライアント装置との間で、第１の鍵を共有するための手続きを行う鍵共有処理手段と、

前記鍵共有処理手段により前記クライアント装置との間で共有された第１の鍵を用いて、送信すべきデータの暗号化又は受信した暗号化データの復号を行う暗号処理手段と、

前記クライアント装置との間で、前記暗号処理手段により暗号化されたデータ又は前記クライアント装置により暗号化されたデータの通信を行う通信手段とを備え、

前記鍵共有処理手段は、

前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを第２の鍵で暗号化した鍵情報を、前記クライアント装置から受信する第１の受信手段と、

前記第２の鍵で暗号化されたデータを復号するのに必要な第３の鍵を保持する鍵管理装置へ、前記鍵情報を復号すべき要求を送信する送信手段と、

前記鍵管理装置から、前記鍵情報を復号して得られた、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを受信する第２の受信手段とを備えることを特徴とするサーバ装置。

【請求項２】

前記第１の鍵を生成するもととなるデータをもとにして、前記第１の鍵を生成する鍵生成手段を更に備えたことを特徴とする請求項１に記載のサーバ装置。

【請求項３】

前記鍵管理装置との間を、前記クライアント装置からは隔離された専用ネットワークを介して接続することを特徴とする請求項１に記載のサーバ装置。

【請求項４】

前記鍵管理装置との間で受け渡しすべきデータを、暗号化して転送することを

特徴とする請求項１に記載のサーバ装置。

【請求項５】

前記鍵管理装置との間で受け渡しすべきデータを暗号化するのに用いる第４の鍵を共有するための手続きとして、前記クライアント装置との間で前記第１の鍵を共有するための手続きと同一のプロトコルに基づく手続きを用いることを特徴とする請求項４に記載のサーバ装置。

【請求項６】

前記送信手段は、予め定められた唯一の鍵管理装置に、前記要求を送信することを特徴とする請求項１に記載のサーバ装置。

【請求項７】

前記送信手段は、予め定められた複数の鍵管理装置のうちから選択した１つの鍵管理装置に、前記要求を送信することを特徴とする請求項１に記載のサーバ装置。

【請求項８】

前記クライアント装置との間でのサーバ認証に用いる情報を保持する手段を更に備えたことを特徴とする請求項１に記載のサーバ装置。

【請求項９】

前記クライアント装置との間でのサーバ認証に用いる情報を、前記鍵管理装置から取得する手段を更に備えたことを特徴とする請求項１に記載のサーバ装置。

【請求項１０】

予め前記第２の鍵を保持し、かつ、いかなる時点においても前記第３の鍵を保持しないことを特徴とする請求項１に記載のサーバ装置。

【請求項１１】

予め前記第２の鍵を保持することなく、かつ、いかなる時点においても前記第３の鍵を保持しないことを特徴とする請求項１に記載のサーバ装置。

【請求項１２】

クライアント装置との間で共有された第１の鍵を用いてデータを暗号化して送受信するサーバ装置から、該第１の鍵を示すデータ又は該第１の鍵を生成するもととなるデータを第２の鍵で暗号化した鍵情報を復号すべき要求を受信する受信

手段と、

前記第２の鍵で暗号化されたデータを復号するのに必要な第３の鍵を保持する保持手段と、

前記要求を受信した場合に、前記第３の鍵で前記鍵情報を復号して、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを求める復号手段と、

前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを、前記サーバ装置へ送信する送信手段とを備えたことを特徴とする鍵管理装置。

【請求項１３】

前記鍵情報は、前記クライアント装置により暗号化されたものであることを特徴とする請求項１２に記載の鍵管理装置。

【請求項１４】

前記サーバ装置との間を、前記クライアント装置からは隔離された専用ネットワークを介して接続することを特徴とする請求項１２に記載の鍵管理装置。

【請求項１５】

前記サーバ装置との間で受け渡しすべきデータを、暗号化して転送することを特徴とする請求項１２に記載の鍵管理装置。

【請求項１６】

前記サーバ装置との間で受け渡しすべきデータを暗号化するのに用いる第４の鍵を共有するための手続きとして、前記サーバ装置と前記クライアント装置との間で前記第１の鍵を共有するための手続きと同一のプロトコルに基づく手続きを用いることを特徴とする請求項１２に記載の鍵管理装置。

【請求項１７】

複数のサーバ装置をサービス対象とし、前記第２の鍵及び第３の鍵を、該サービス対象とする複数のサーバ装置に共通とすることを特徴とする請求項１２に記載の鍵管理装置。

【請求項１８】

複数のサーバ装置をサービス対象とし、前記第２の鍵及び第３の鍵を、該サービス対象とする各サーバ装置ごとに固有に設けることを特徴とする請求項１２に

記載の鍵管理装置。

【請求項１９】

前記サーバ装置が前記クライアント装置との間でのサーバ認証に用いる情報を保持する手段と、

前記サーバ装置から前記サーバ認証に用いる情報の要求を受信する手段と、

前記要求を受信した場合に、前記サーバ認証に用いる情報を、前記サーバ装置に送信する手段とを更に備えたことを特徴とする請求項１２に記載の鍵管理装置。

【請求項２０】

クライアント装置との間で、第１の鍵を共有するための手続きを行う鍵共有処理ステップと、

前記鍵共有処理ステップにより前記クライアント装置との間で共有された第１の鍵を用いて、送信すべきデータの暗号化又は受信した暗号化データの復号を行う暗号処理ステップと、

前記クライアント装置との間で、前記暗号処理ステップにより暗号化されたデータ又は前記クライアント装置により暗号化されたデータの通信を行う通信ステップとを有し、

前記鍵共有処理ステップは、

前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを第２の鍵で暗号化した鍵情報を、前記クライアント装置から受信する第１の受信ステップと、

前記第２の鍵で暗号化されたデータを復号するのに必要な第３の鍵を保持する鍵管理装置へ、前記鍵情報を復号すべき要求を送信する送信ステップと、

前記鍵管理装置から、前記鍵情報を復号して得られた、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを受信する第２の受信ステップとを含むことを特徴とする暗号通信方法。

【請求項２１】

クライアント装置との間で共有された第１の鍵を用いてデータを暗号化して送受信するサーバ装置から、該第１の鍵を示すデータ又は該第１の鍵を生成するも

ととなるデータを第２の鍵で暗号化した鍵情報を復号すべき要求を受信する受信ステップと、

前記第２の鍵で暗号化されたデータを復号するのに必要な第３の鍵を保持する保持ステップと、

前記要求を受信した場合に、前記第３の鍵で前記鍵情報を復号して、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを求める復号ステップと、

前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを、前記サーバ装置へ送信する送信ステップとを有することを特徴とする暗号通信方法。

【請求項２２】

コンピュータをサーバ装置として機能させるためのプログラムであって、

クライアント装置との間で、第１の鍵を共有するための手続きを行う鍵共有処理機能と、

前記鍵共有処理機能により前記クライアント装置との間で共有された第１の鍵を用いて、送信すべきデータの暗号化又は受信した暗号化データの復号を行う暗号処理機能と、

前記クライアント装置との間で、前記暗号処理機能により暗号化されたデータ又は前記クライアント装置により暗号化されたデータの通信を行う通信機能とを実現させ、

前記鍵共有処理機能は、

前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを第２の鍵で暗号化した鍵情報を、前記クライアント装置から受信する第１の受信機能と、

前記第２の鍵で暗号化されたデータを復号するのに必要な第３の鍵を保持する鍵管理装置へ、前記鍵情報を復号すべき要求を送信する送信機能と、

前記鍵管理装置から、前記鍵情報を復号して得られた、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを受信する第２の受信機能とを含むことを特徴とするプログラム。

【請求項２３】

コンピュータを鍵管理装置として機能させるためのプログラムであって、

クライアント装置との間で共有された第１の鍵を用いてデータを暗号化して送受信するサーバ装置から、該第１の鍵を示すデータ又は該第１の鍵を生成するもととなるデータを第２の鍵で暗号化した鍵情報を復号すべき要求を受信する受信機能と、

前記第２の鍵で暗号化されたデータを復号するのに必要な第３の鍵を保持する保持機能と、

前記要求を受信した場合に、前記第３の鍵で前記鍵情報を復号して、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを求める復号機能と、

前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを、前記サーバ装置へ送信する送信機能とを実現させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号通信を行うサーバ装置、暗号通信に用いる共通鍵を得るための秘密の鍵を管理する鍵管理装置、暗号通信方法及びプログラムに関する。

【０００２】

【従来の技術】

インターネットやＬＡＮなどのネットワークで接続された計算機間で通信を行う場合、その通信内容の盗聴や改竄等を防止するために、ＳＳＬ(Secure Sockets Layer)と呼ぶ技術が広く用いられている（例えば、非特許文献１参照）。

【０００３】

２つの計算機上のアプリケーションが通信する場合、各アプリケーションは、ソケットなどのインターフェースを使って、ＴＣＰ／ＩＰなどの通信機能を呼び出す。ネットワークを流れるパケットが暗号化されていないと、盗聴や改竄等の危険性が伴う。これに対して、ＳＳＬを使って通信する場合は、アプリケーションプログラムとＴＣＰ／ＩＰ処理部との間にＳＳＬ処理部が入る。ＳＳＬ処理部

では、アプリケーションプログラムが送信するデータを暗号化してネットワークに送り出し、また、ネットワークから受信したデータを復号してアプリケーションプログラムに渡す。

【０００４】

ＳＳＬ処理部は、ＯＳの機能としてＴＣＰ／ＩＰ処理部の上層に実装される場合もあるし、プログラムライブラリの形態でアプリケーションプログラムにリンクするように実装される場合もある。

【０００５】

また、ＳＳＬ処理部を別の計算機上に実装する場合もある。例えば、計算機＃１と計算機＃３の間の通信は暗号化されるが、計算機＃３と計算機＃２との間の通信は暗号化しないような使い方においては、計算機＃２がＳＳＬに対応していない場合でも、計算機＃２と計算機＃３との間のネットワークを隔離して保護することで、計算機＃１との間の通信を暗号化することができる。ここでは、計算機＃３にＳＳＬの機能を持たせたが、計算機＃３の機能をハードウェア化する実装も可能である。

【０００６】

ＳＳＬを使った典型的な通信は、ＷＥＢブラウザとＷＥＢサーバのようなクライアント計算機とサーバ計算機との間の通信である。

【０００７】

【非特許文献１】

「インターネット暗号化技術 ～PKI, RSA, SSL, S/MIME, etc～」、 岩田彰監修、 鈴木春洋　他　著、株式会社ソフト・リサーチ・センター発行、ＩＳＢＮ：４－８８３７３－１６６－９

【０００８】

【発明が解決しようとする課題】

大規模なＷＥＢサイトに代表されるように、インターネット上で同時に多数のユーザに対してサービスを提供する場合、複数台のサーバ計算機を用いて負荷を分散させたり、耐障害性を向上させることが多い。このとき、クライアント計算機とサーバ計算機との間の通信にＳＳＬを用いようとすると、すべてのサーバ計

算機のＳＳＬ処理部が秘密鍵と証明書を持つ必要がある。

【０００９】

しかし、秘密鍵を複数のサーバ計算機上に持つことは、安全性の観点から望ましくない。すなわち、秘密鍵を複数の計算機に配布すると、その配布経路で秘密鍵が漏洩する危険性を伴う。また、遠隔地にある計算機はそれぞれ別の人が管理していることが多く、それだけ秘密鍵にアクセス可能な人が多くなるので、秘密鍵が漏洩する危険性は増大する。さらに、一時的な負荷の増大に対処するためにサーバを借りるような利用法では、そのサーバの使用中に秘密鍵を盗み見られたり、あるいは使用後のメモリの状態等から秘密鍵が漏洩する危険性がある。

【００１０】

本発明は、上記事情を考慮してなされたもので、秘密鍵に関する安全性をより高めたサーバ装置、鍵管理装置、暗号通信方法及びプログラムを提供することを目的とする。

【００１１】

【課題を解決するための手段】

本発明に係るサーバ装置は、クライアント装置との間で、第１の鍵を共有するための手続きを行う鍵共有処理手段と、前記鍵共有処理手段により前記クライアント装置との間で共有された第１の鍵を用いて、送信すべきデータの暗号化又は受信した暗号化データの復号を行う暗号処理手段と、前記クライアント装置との間で、前記暗号処理手段により暗号化されたデータ又は前記クライアント装置により暗号化されたデータの通信を行う通信手段とを備え、前記鍵共有処理手段は、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを第２の鍵で暗号化した鍵情報を、前記クライアント装置から受信する第１の受信手段と、前記第２の鍵で暗号化されたデータを復号するのに必要な第３の鍵を保持する鍵管理装置へ、前記鍵情報を復号すべき要求を送信する送信手段と、前記鍵管理装置から、前記鍵情報を復号して得られた、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを受信する第２の受信手段とを備えることを特徴とする。

【００１２】

本発明に係る鍵管理装置は、クライアント装置との間で共有された第１の鍵を用いてデータを暗号化して送受信するサーバ装置から、該第１の鍵を示すデータ又は該第１の鍵を生成するもととなるデータを第２の鍵で暗号化した鍵情報を復号すべき要求を受信する受信手段と、前記第２の鍵で暗号化されたデータを復号するのに必要な第３の鍵を保持する保持手段と、前記要求を受信した場合に、前記第３の鍵で前記鍵情報を復号して、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを求める復号手段と、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを、前記サーバ装置へ送信する送信手段とを備えたことを特徴とする。

【００１３】

本発明に係る暗号通信方法は、クライアント装置との間で、第１の鍵を共有するための手続きを行う鍵共有処理ステップと、前記鍵共有処理ステップにより前記クライアント装置との間で共有された第１の鍵を用いて、送信すべきデータの暗号化又は受信した暗号化データの復号を行う暗号処理ステップと、前記クライアント装置との間で、前記暗号処理ステップにより暗号化されたデータ又は前記クライアント装置により暗号化されたデータの通信を行う通信ステップとを有し、前記鍵共有処理ステップは、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを第２の鍵で暗号化した鍵情報を、前記クライアント装置から受信する第１の受信ステップと、前記第２の鍵で暗号化されたデータを復号するのに必要な第３の鍵を保持する鍵管理装置へ、前記鍵情報を復号すべき要求を送信する送信ステップと、前記鍵管理装置から、前記鍵情報を復号して得られた、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを受信する第２の受信ステップとを含むことを特徴とする。

【００１４】

また、本発明に係る暗号通信方法は、クライアント装置との間で共有された第１の鍵を用いてデータを暗号化して送受信するサーバ装置から、該第１の鍵を示すデータ又は該第１の鍵を生成するもととなるデータを第２の鍵で暗号化した鍵情報を復号すべき要求を受信する受信ステップと、前記第２の鍵で暗号化されたデータを復号するのに必要な第３の鍵を保持する保持ステップと、前記要求を受

信した場合に、前記第３の鍵で前記鍵情報を復号して、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを求める復号ステップと、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを、前記サーバ装置へ送信する送信ステップとを有することを特徴とする。

【００１５】

また、本発明は、コンピュータをサーバ装置として機能させるためのプログラムであって、クライアント装置との間で共有された第１の鍵を用いてデータを暗号化して送受信するサーバ装置から、該第１の鍵を示すデータ又は該第１の鍵を生成するもととなるデータを第２の鍵で暗号化した鍵情報を復号すべき要求を受信する受信機能と、前記第２の鍵で暗号化されたデータを復号するのに必要な第３の鍵を保持する保持機能と、前記要求を受信した場合に、前記第３の鍵で前記鍵情報を復号して、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを求める復号機能と、前記第１の鍵を示すデータ又は前記第１の鍵を生成するもととなるデータを、前記サーバ装置へ送信する送信機能とを実現させるためのプログラムである。

【００１６】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【００１７】

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００１８】

本発明によれば、秘密鍵を限定された箇所で管理できるので、秘密鍵に関する安全性をより高めることができる。この結果、例えば、ＳＳＬで通信するサーバ計算機を分散・並列化する際の安全性がより高まる。

【００１９】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【００２０】

図１に、本発明の一実施形態に係る通信システムの構成例を示す。

【００２１】

図１に示されるように、複数のサーバ計算機１と、キーサーバ３と、クライアント計算機５が、ネットワーク７に接続可能になっている。

【００２２】

サーバ計算機１は、アプリケーションプログラムを実行するためのアプリケーションプログラム実行部１１、ＳＳＬ処理（鍵を共有するための手続き並びに送信すべきデータの暗号化及び受信した暗号化データの復号など）を行うＳＳＬ処理部１２、ＴＣＰ／ＩＰ処理を行うＴＣＰ／ＩＰ処理部１３、証明書（含む公開鍵）を格納するための証明書格納部１４を備えている（証明書格納部１４は、ＳＳＬ処理部１２内に存在してもよい）。

【００２３】

キーサーバ３は、秘密鍵の管理を行う秘密鍵管理部３１、ＴＣＰ／ＩＰ処理を行うＴＣＰ／ＩＰ処理部３２、秘密鍵を格納するための秘密鍵格納部３３を備えている（秘密鍵格納部３３は、秘密鍵管理部３１内に存在してもよい）。

【００２４】

クライアント計算機５は、アプリケーションプログラムを実行するためのアプリケーションプログラム実行部５１、ＳＳＬ処理を行うＳＳＬ処理部５２、ＴＣＰ／ＩＰ処理を行うＴＣＰ／ＩＰ処理部５３を備えている。

【００２５】

本実施形態では、図１に示すように、「秘密鍵」は、キーサーバ３のみが管理するようにしており、ＳＳＬを使って通信する各サーバ計算機１は秘密鍵を持たないようにしている。

【００２６】

本実施形態のサーバ計算機１は、基本的には、従来のものと同様の機能を有するものであるが、従来と異なり自身では秘密鍵を保持・管理しないので、秘密鍵

を持つキーサーバ３に対して、秘密鍵に基づく処理を要求し、その結果を取得するための機能を有している。

【００２７】

本実施形態のキーサーバ３は、従来、存在しないもので、サーバ計算機１からの要求に応答して、秘密鍵に基づく処理を行い、その結果を返すための機能を有している。

【００２８】

本実施形態のクライアント計算機５は、従来と同様のもので構わない。

【００２９】

なお、図１の例では、３台のサーバ計算機１が接続されているが、もちろん、これは一例であり、サーバ計算機１の台数は任意である。また、図１の例では、１台のクライアント計算機５のみが示されているが、もちろん、クライアント計算機５は複数台存在し得る。

【００３０】

以下では、キーサーバ３は１台のみ存在し、すべてのサーバ計算機１はそのキーサーバ３に対して秘密鍵に基づく処理を要求し、そのキーサーバ３は複数のサーバ計算機１のすべてに共通に唯一の秘密鍵を用いる場合を例にとって説明する。

【００３１】

図２に、本実施形態においてクライアント計算機５とサーバ計算機１とがＳＳＬを用いた通信を開始するにあたって行われる手順の一例を示す。図２では、クライアント計算機５とサーバ計算機１との間（ＳＳＬ処理部１２，５２間）及びサーバ計算機１・キーサーバ３間（ＳＳＬ処理部１２・秘密鍵管理部３１間）のプロトコルを示している。

【００３２】

クライアント計算機５が複数のサーバ計算機１のうちのあるサーバ計算機（例えば、図１の＃１のサーバ計算機とする（以下の処理は他のサーバ計算機でも同様である））との間でＳＳＬを用いた通信を始める際は、まず、以降の通信に使うキーの種の一部になるクライアント乱数（ＣＲ）を生成する（ステップＳ５１

）。

【００３３】

そして、クライアント計算機５は、ＣｌｉｅｎｔＨｅｌｌｏメッセージに、生成したＣＲと、受け入れ可能な暗号化方式のペアリスト（キーの交換に使う暗号化方式と、通信データの転送に使う暗号化方式とのペアを１又は複数ペア記述したリスト）とを付けて、サーバ計算機（＃１）送る（ステップＳ１）。

【００３４】

このＣｌｉｅｎｔＨｅｌｌｏメッセージを受け取った（ステップＳ１）サーバ計算機（＃１）は、ＣＲと同様に以降の通信に使うキーの種の一部になるサーバ乱数（ＳＲ）を生成するとともに（ステップＳ１１）、送られてきた暗号化方式のペアリストの中から以降の通信に用いる暗号化方式を選択し、ＳｅｒｖｅｒＨｅｌｌｏメッセージに、生成したＳＲと、選択した暗号化方式とを付けて、クライアント計算機５へ送る（ステップＳ２）。次いで、サーバ計算機（＃１）は、ＳｅｒｖｅｒＣｅｒｔｉｆｉｃａｔｅメッセージに、自身の持っている証明書（図１の１４参照）を付けて、クライアント計算機５へ送り（ステップＳ３）、さらに、ＳｅｒｖｅｒＨｅｌｌｏＤｏｎｅメッセージをクライアント計算機５へ送る（ステップＳ４）。

【００３５】

クライアント計算機１は、サーバ計算機（＃１）から、ＳｅｒｖｅｒＨｅｌｌｏメッセージ（ステップＳ２）、ＳｅｒｖｅｒＣｅｒｔｉｆｉｃａｔｅメッセージ（ステップＳ３）、ＳｅｒｖｅｒＨｅｌｌｏＤｏｎｅメッセージ（ステップＳ４）を順次受けると、以降の通信に使うキーの種の一部になるプレマスタシークレット（ＰＳ）と呼ぶ乱数を生成し（ステップＳ５２）、それを、サーバ計算機（＃１）から送られてきたＳｅｒｖｅｒＣｅｒｔｉｆｉｃａｔｅメッセージ（ステップＳ３）に付加されている証明書の中にある公開鍵で暗号化し、これを、ＣｌｉｅｎｔＫｅｙＥｘｃｈａｎｇｅメッセージに付けて、サーバ計算機（＃１）に送る（ステップＳ５）。

【００３６】

ここで、ＰＳを復号するためには秘密鍵が必要であるが、本実施形態では、サ

ーバ計算機１には秘密鍵を持たせないようにしているので、サーバ計算機１が自身ではＰＳを復号することができない。そして、本実施形態では、サーバ計算機１は、秘密鍵によるＰＳの復号について、キーサーバ３によるサポートを受けるようにしている。すなわち、サーバ計算機１のＳＳＬ処理部１２は、復号するためには秘密鍵を必要とするようなデータを受け取ると、そのデータをキーサーバ３に渡して復号してもらうように動作し、キーサーバ３の秘密鍵管理部３１は、サーバ計算機１のＳＳＬ処理部１２から受け取ったデータを、自身の管理している秘密鍵（図１の３３参照）で復号して送り返すように動作する。

【００３７】

さて、図２の例においては、サーバ計算機（＃１）は、クライアント計算機５からＣｌｉｅｎｔＫｅｙＥｘｃｈａｎｇｅメッセージを受けると（ステップＳ６）、このＣｌｉｅｎｔＫｅｙＥｘｃｈａｎｇｅメッセージに付加されている公開鍵で暗号化されたＰＳを、復号を要求する復号要求メッセージに付加して、キーサーバ３へ送る（ステップＳ６）。

【００３８】

復号要求メッセージを受信した（ステップＳ６）キーサーバ３は、該復号要求メッセージに付加されている公開鍵で暗号化されたＰＳを、自身の管理している秘密鍵（図１の３３参照）で復号し（ステップＳ３１）、これによって得られたＰＳを、復号要求メッセージに対する応答メッセージに付加して、要求元のサーバ計算機（＃１）へ返す（ステップＳ７）。

【００３９】

復号要求メッセージに対する応答メッセージを受信した（ステップＳ７）サーバ計算機（＃１）は、既に取得しているＣＲと（ステップＳ１）、既に生成しているＳＲと（ステップＳ１１）と、該応答メッセージに付加されているＰＳとの３つの乱数を種として、マスターシークレット（ＭＳ）と呼ばれる数を計算する（ステップＳ１２）。その後、ＭＳを種として所定の手順で、キーブロックと呼ばれる数の列を作る（ステップＳ１３）。そして、これを基にして、データの通信に必要な共通鍵などを作り出す。

【００４０】

他方、クライアント計算機５は、ステップＳ５２でＰＳを生成した時点で、３つの乱数が揃うので、それ以降の適当なタイミングで、同様に、ＣＲとＳＲとＰＳとの３つの乱数を種として、ＭＳを計算する（ステップＳ５３）。また、その後、同様に、ＭＳを種として所定の手順で、キーブロックと呼ばれる数の列を作る（ステップＳ５４）。そして、これを基にして、データの通信に必要な共通鍵などを作り出す。

【００４１】

しかして、クライアント計算機５からはＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃメッセージとＦｉｎｉｓｈｅｄメッセージが順次サーバ計算機（＃１）へ送られ（ステップＳ８，Ｓ９）、他方、サーバ計算機（＃１）からもＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃメッセージとＦｉｎｉｓｈｅｄメッセージが順次クライアント計算機５へ送られ（ステップＳ１０，Ｓ１１）、ＳＳＬを使った通信の確立フェーズが完了する。

【００４２】

以降は、それまでに決定した暗号化方式と共通鍵を使って、クライアント計算機とサーバ計算機の間でデータの通信を行う（ステップＳ１２）。

【００４３】

なお、以上に示した手順例は、サーバ認証のみを行う場合のＳＳＬを使った通信の例であるが、クライアント計算機１にも秘密鍵と証明書を持たせてクライアント認証をも行うような場合にもサーバ認証について同様の手順を用いることができる（クライアント認証の部分は、従来通りでもよいし、サーバ認証と同様にクライアント計算機をサポートするキーサーバを設けてもよい）。

【００４４】

また、図１に示すようにサーバの証明書を全サーバ計算機１が持つように実施してもよいし、全サーバ計算機１とキーサーバ３のそれぞれが持つように実施してもよいし、あるいは、図３のようにキーサーバ３のみが証明書（図３の３４参照）を持っていて（あるいは、キーサーバ３と一部のサーバ計算機１のみが証明書を持っていて）、（証明書を持たない）サーバ計算機１は、例えば、証明書が必要になるごと、毎回、キーサーバからもらうようにしてもよいし、毎回、キー

サーバからもらうのではなく、所定のタイミングで（例えば、有効な証明書を保持しない状態で最初に証明書が必要になったとき、あるいは、起動してから所定時間経過したとき、など）、一度、キーサーバからもらった証明書を、サーバ計算機１がキャッシュして使うようにしてもよい。

【００４５】

また、上記では、（１）キーサーバ３は１台のみ存在し、すべてのサーバ計算機１はそのキーサーバ３に対して秘密鍵に基づく処理を要求し、そのキーサーバ３は複数のサーバ計算機１のすべてに共通に唯一の秘密鍵を用いる場合を例にとって説明したが、（２）キーサーバ３は複数台存在し、各サーバ計算機１はいずれか１台のキーサーバ３に対して秘密鍵に基づく処理を要求し、そのキーサーバ３は自身がサポートしているサーバ計算機１のすべてに共通に唯一の秘密鍵を用いる構成や、（３）キーサーバ３は複数台存在し、各サーバ計算機１は予め定められた（全部又は一部の）キーサーバ３のうちのいずれかに対して秘密鍵に基づく処理を要求することができ（複数台のキーサーバからサポートを受けるサーバ計算機１は、例えば、要求時に、いずれか１台のキーサーバ３を選択して、要求を行えばよい）、そのキーサーバ３は自身がサポートしているサーバ計算機１のすべてに共通に唯一の秘密鍵を用いる構成や、そららの他の構成も可能である。また、上記の（１）、（２）、（３）や、それら他の構成において、キーサーバ３は、要求元のサーバ計算機１ごとに固有の秘密鍵を持ち、サーバ計算機１から要求を受けたときは、当該要求元のサーバ計算機１に対応する秘密鍵を用いるようにしてもよい。

【００４６】

（２）のように複数のキーサーバを設置することで、キーサーバの負荷を軽減したり、故障の影響を一部の範囲にとどめたりすることができる。

【００４７】

（３）のように複数のキーサーバを設置して多重化することで、耐障害性を高めることができる。

【００４８】

また、通信システム中に、本実施形態のサーバ計算機１とともに、従来のよう

に自身で秘密鍵（例えばキーサーバ３が管理する秘密鍵とは異なる独自の秘密鍵）を持ってキーサーバ３のサポートは受けないでＳＳＬを行うサーバ計算機や、本実施形態のサーバ計算機１のようにキーサーバ３のサポートを受けてＳＳＬを行う機能と従来のように自身で秘密鍵（例えばキーサーバ３が管理する秘密鍵とは異なる独自の秘密鍵）を持ってキーサーバ３のサポートは受けないでＳＳＬを行う機能とを使い分けることのできるサーバ計算機などが、混在していても構わない。

【００４９】

ところで、本実施形態において、サーバ計算機１とキーサーバ３との間の通信が傍受されてＰＳが盗まれないようにするのは望ましい。

【００５０】

これを防ぐためには、種々の方法が考えられるが、例えば、サーバ計算機１とキーサーバ３との間のネットワークを、少なくともクライアント計算機５からは隔離された専用ネットワークにする方法がある。

【００５１】

また、他の方法としては、例えば、サーバ計算機１とキーサーバ３との間のネットワークを、クライアント計算機５から接続可能なネットワーク（例えば、図１のネットワーク７）とする場合であっても、図４に示すように、キーサーバ３もＳＳＬ処理部３５を備え、サーバ計算機１とキーサーバ３との間の通信にもＳＳＬを使うことによって、暗号化されたＰＳ（を含む復号要求メッセージ）の通信や、復号したＰＳ（を含む応答メッセージの通信）を保護することもできる。この場合、サーバ計算機１とキーサーバ３との間の通信は、従来のクライアント計算機とサーバ計算機との間のＳＳＬを使った通信と同様に実現することができる。もちろん、サーバ計算機１とキーサーバ３との間のネットワークを、少なくともクライアント計算機５からは隔離された専用ネットワークにする場合においても、サーバ計算機１とキーサーバ３との間の通信を、従来のクライアント計算機とサーバ計算機との間のＳＳＬを使った通信と同様に実現するようにしてもよい。

【００５２】

なお、図４は、（１）クライアント計算機５とサーバ計算機１との間のデータ通信のためのＳＳＬで使用する秘密鍵Ａ（すなわち、クライアント計算機５が暗号化したＰＳの復号化に用いる鍵）と、サーバ計算機１とキーサーバ３との間のＳＳＬで使用する秘密鍵Ｂ（すなわち、サーバ計算機１が暗号化したＰＳの復号化に用いる鍵）とのすべてに、同一の秘密鍵（図４の３３参照）を使用する場合を例示しているが、（２）秘密鍵Ａはサーバ計算機にかかわらずにすべて同一であるが、秘密鍵Ａと秘密鍵Ｂとは異なるものにする方法もある。また、（３）秘密鍵Ａをサーバ計算機ごとに設ける場合には、秘密鍵Ｂは、秘密鍵Ａのいずれとも異なるものにする方法と、秘密鍵Ａのいずれかと一致しても構わないものとする方法などがある。

【００５３】

また、キーサーバ３が複数存在する構成を採用する場合において、これまでの考え方をキーサーバ３にも適用し、キーサーバ３には、秘密鍵Ｂを持たせず、秘密鍵Ｂを管理する（キーサーバ３に対する）キーサーバを設けるようにすることも可能である。

【００５４】

また、この場合において、キーサーバ３には、秘密鍵Ａをも持たせず、（キーサーバ３に対する）キーサーバに、秘密鍵Ａをも管理させるようにすることも可能である。この構成においては、キーサーバ３は、サーバ計算機１から復号要求メッセージを受信すると、さらに、（キーサーバ３に対する）キーサーバへ、復号要求メッセージを送信し、復号要求メッセージを受信した（キーサーバ３に対する）キーサーバは、ＰＳを復号して、これを含む応答メッセージを、要求元のキーサーバへ返送し、これを受信したキーサーバ３は、さらに、要求元のサーバ装置１へ、ＰＳを含む応答メッセージを返送するようにしてもよい。

【００５５】

また、本実施形態では、ＳＳＬを使った通信として、ＷＥＢブラウザとＷＥＢサーバのようなクライアント計算機とサーバ計算機との間の通信を例にとって説明してが、もちろん、計算機が、クライアント計算機やサーバ計算機以外の計算機であっても構わない。また、計算機が、例えば携帯電話等の端末装置であって

も構わない。

【００５６】

また、本実施形態は、図１のような分散したサーバ計算機をターゲットにしたときだけでなく、ＳＳＬの処理を行う計算機あるいはＳＳＬアクセラレータとよばれる専用ハードウェアを複数台束ねて性能を高める際にも、それぞれの計算機あるいは専用ハードウェアに秘密鍵を配るのではなく、キーサーバで秘密鍵を一元的に管理するために用いることができる。

【００５７】

また、本実施形態は、サーバ計算機の側のみに証明書と秘密鍵を持たせるＳＳＬの使い方を中心に説明しているが、クライアントにも証明書を持たせてクライアント認証もするようなＳＳＬの使い方においても同様に実施することができる。

【００５８】

また、本実施形態は、ＳＳＬを対象にして記述しているが、ＳＳＬと類似の技術であるＴＬＳ(Transport Layer Security)など、他のプロトコルに対しても同様に実施することができる。

【００５９】

また、例えば、クライアント側で共通鍵を生成し、クライアントからサーバへ、公開鍵で暗号化した共通鍵を転送するようなプロトコルに対しても本実施形態は適用可能である。

【００６０】

本実施形態によれば、秘密鍵をサーバ計算機に持たせないので、サーバ計算機自体から秘密鍵が漏洩する危険性がない。また、サーバ計算機への秘密鍵の配布経路がないので、配布経路で秘密鍵が漏洩する危険を回避できる。また、秘密鍵にアクセス可能な人が限定されるので、秘密鍵が漏洩する危険性を極めて低減させることができる。

【００６１】

なお、以上の各機能は、ソフトウェアとして実現可能である。

【００６２】

また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムとして実施することもでき、該プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。

【００６３】

なお、この発明の実施の形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能あるいは要素を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。

【００６４】

また、この発明の実施の形態で例示した各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。

また、この発明の実施の形態は、個別装置としての発明、関連を持つ２以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。

従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【００６５】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【００６６】

【発明の効果】

本発明は、秘密鍵に関する安全性をより高めることができる。

【図面の簡単な説明】

【図１】　本発明の一実施形態に係る通信システムの構成例を示す図

【図２】　同実施形態に係る通信システムの処理手順の一例を示す図

【図３】　実施形態に係る通信システムの他の構成例を示す図

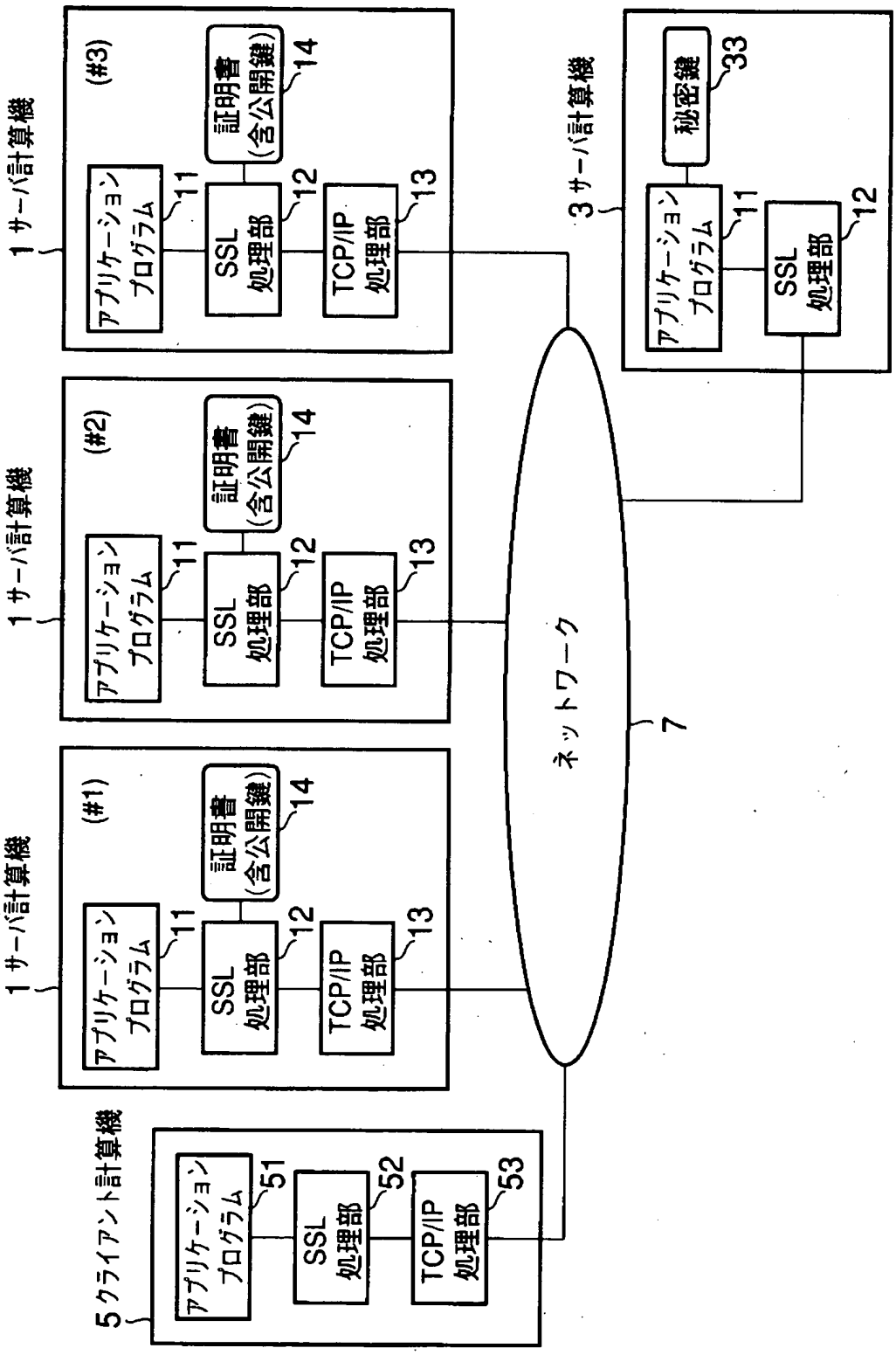
【図４】　実施形態に係る通信システムのさらに他の構成例を示す図

【符号の説明】

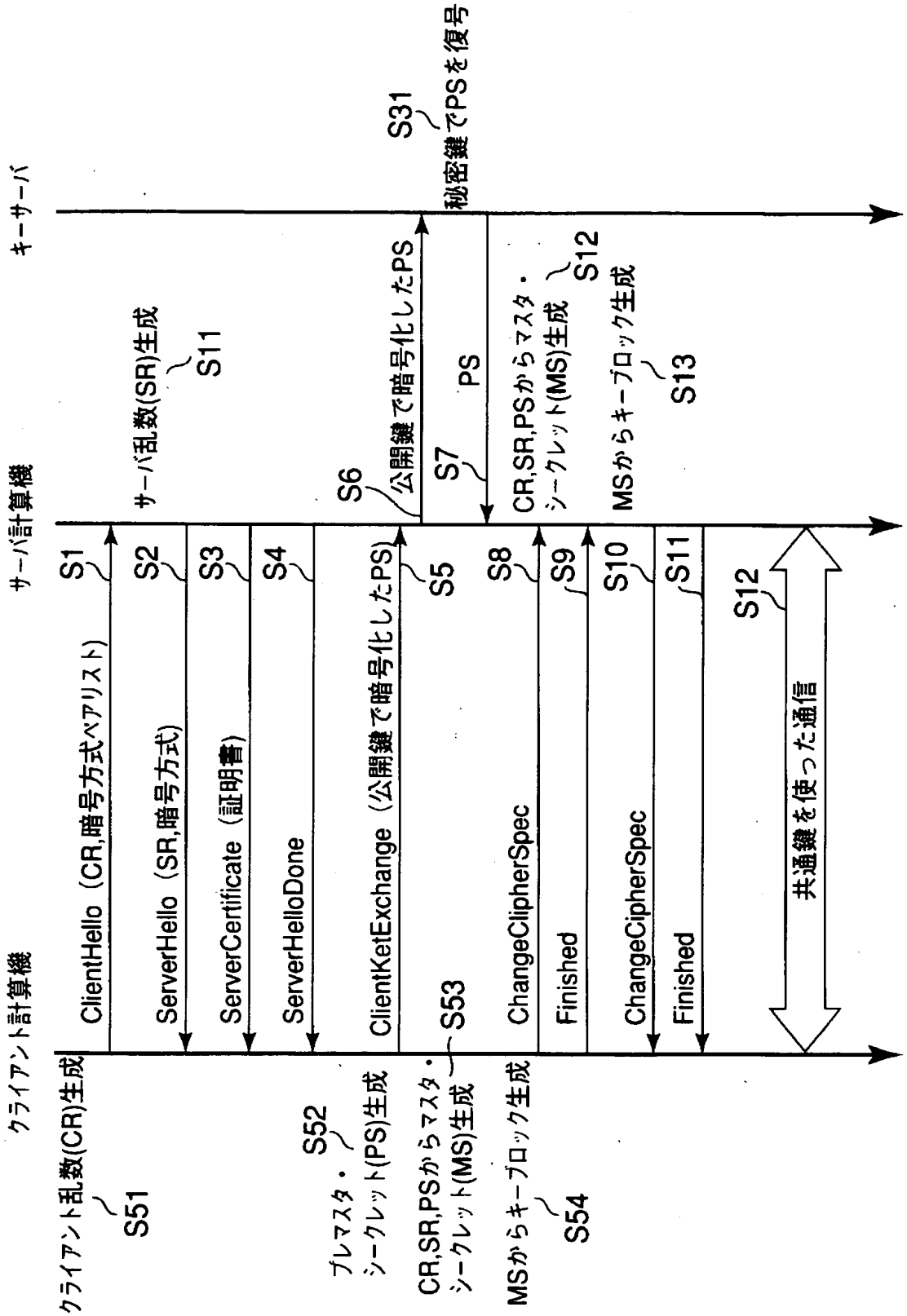
１…サーバ計算機、３…キーサーバ、５…クライアント計算機、７…ネットワーク、１１，５１…アプリケーションプログラム実行部、１２，３５，５２…ＳＳＬ処理部、１３，３２，５３…ＴＣＰ／ＩＰ処理部、１４，３４…証明書格納部、３１，３３…秘密鍵管理部

【書類名】　図面

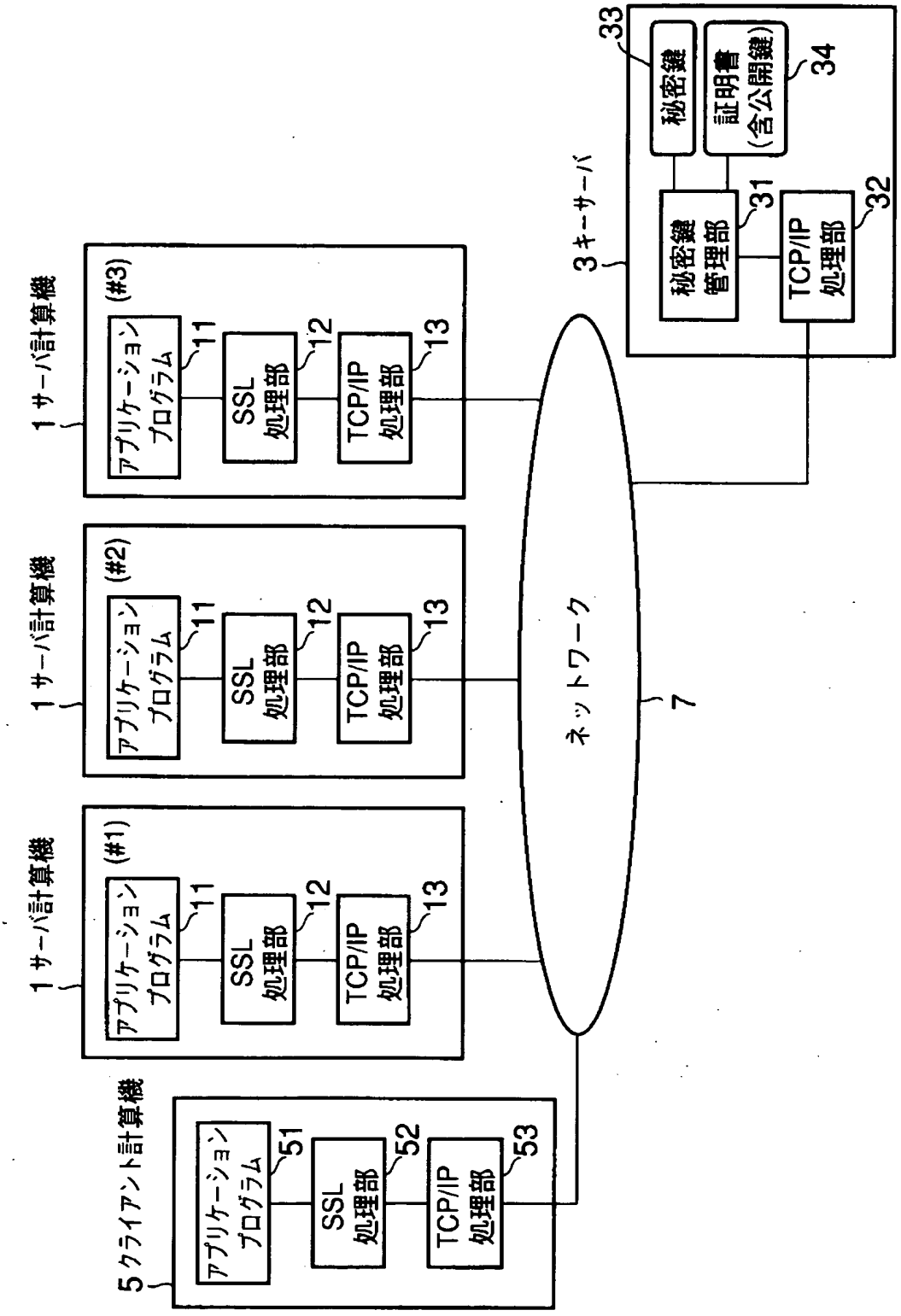
【図１】


1サーバ計算機
(#3)
アプリケーション プログラム
11
SSL 処理部
12
TCP/IP 処理部
13
証明書 (含公開鍵)
14
1サーバ計算機
(#2)
アプリケーション プログラム
11
SSL 処理部
12
TCP/IP 処理部
13
証明書 (含公開鍵)
14
1サーバ計算機
(#1)
アプリケーション プログラム
11
SSL 処理部
12
TCP/IP 処理部
13
証明書 (含公開鍵)
14
3サーバ計算機
アプリケーション プログラム
11
SSL 処理部
12
秘密鍵
33
ネットワーク
7
5クライアント計算機
アプリケーション プログラム
51
SSL 処理部
52
TCP/IP 処理部
53

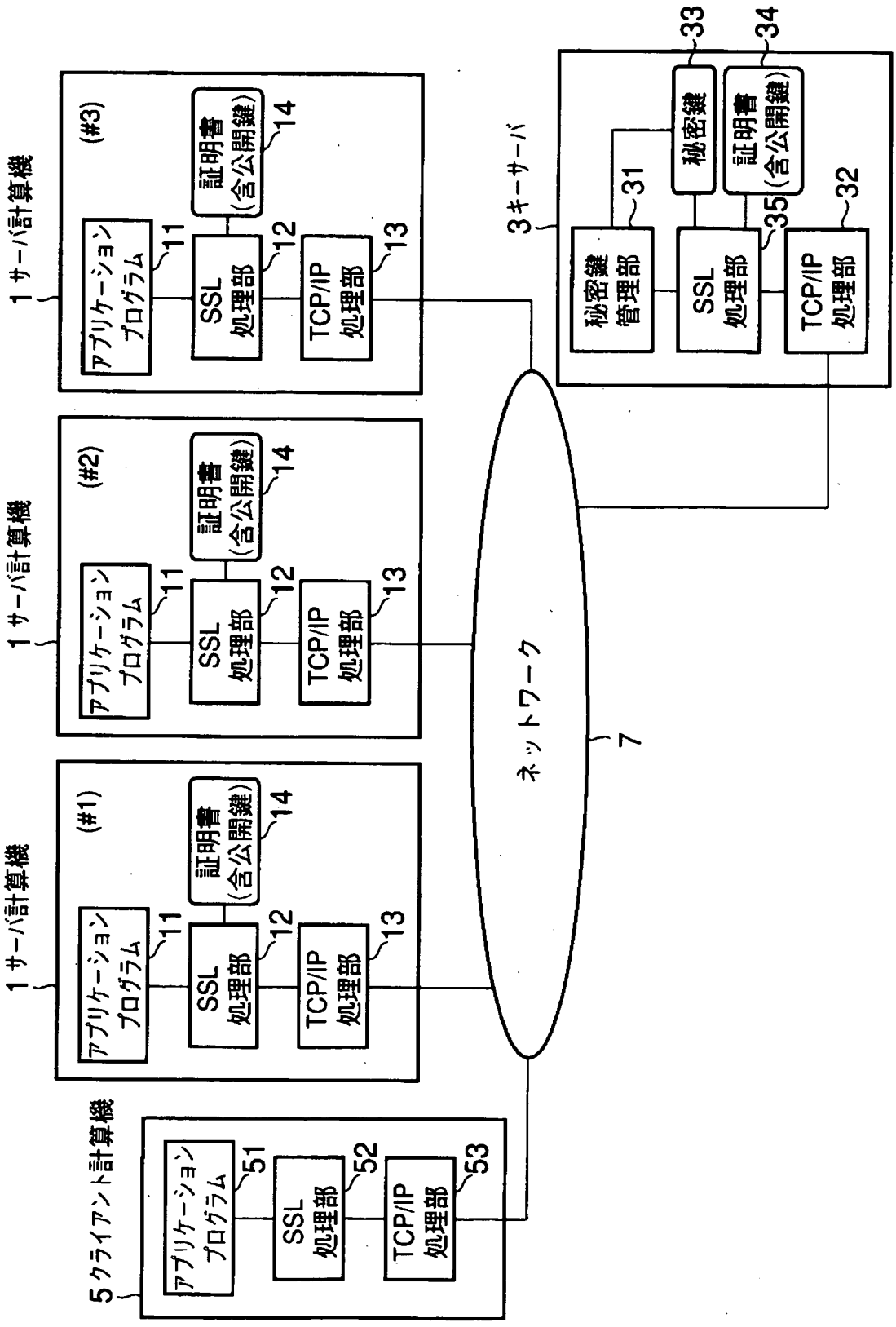
【図２】


クライアント計算機
サーバ計算機
キーサーバ
クライアント乱数(CR)生成
S51
ClientHello（CR,暗号方式ペアリスト）
S1
ServerHello（SR,暗号方式）
S2
ServerCertificate（証明書）
S3
ServerHelloDone
S4
プレマスタ・シークレット(PS)生成
S52
ClientKetExchange（公開鍵で暗号化したPS）
S5
CR,SR,PSからマスタ・シークレット(MS)生成
S53
ChangeCliperSpec
S8
Finished
S9
MSからキーブロック生成
S54
ChangeCipherSpec
S10
Finished
S11
共通鍵を使った通信
S12
サーバ乱数(SR)生成
S11
公開鍵で暗号化したPS
S6
PS
S7
秘密鍵でPSを復号
S31
CR,SR,PSからマスタ・シークレット(MS)生成
S12
MSからキーブロック生成
S13

【図３】


1サーバ計算機
(#3)
アプリケーション プログラム
11
SSL 処理部
12
TCP/IP 処理部
13
1サーバ計算機
(#2)
アプリケーション プログラム
11
SSL 処理部
12
TCP/IP 処理部
13
1サーバ計算機
(#1)
アプリケーション プログラム
11
SSL 処理部
12
TCP/IP 処理部
13
ネットワーク
7
3キーサーバ
秘密鍵
33
証明書 (含公開鍵)
34
秘密鍵 管理部
31
TCP/IP 処理部
32
5クライアント計算機
アプリケーション プログラム
51
SSL 処理部
52
TCP/IP 処理部
53

【図４】


1サーバ計算機
(#3)
アプリケーション プログラム
11
SSL 処理部
12
TCP/IP 処理部
13
証明書 (含公開鍵)
14
1サーバ計算機
(#2)
アプリケーション プログラム
11
SSL 処理部
12
TCP/IP 処理部
13
証明書 (含公開鍵)
14
1サーバ計算機
(#1)
アプリケーション プログラム
11
SSL 処理部
12
TCP/IP 処理部
13
証明書 (含公開鍵)
14
5クライアント計算機
アプリケーション プログラム
51
SSL 処理部
52
TCP/IP 処理部
53
ネットワーク
7
3キーサーバ
秘密鍵管理部
31
秘密鍵
33
SSL 処理部
35
TCP/IP 処理部
32
証明書 (含公開鍵)
34

【書類名】　　要約書

【要約】

【課題】　秘密鍵に関する安全性をより高めたサーバ装置を提供すること。

【解決手段】　サーバ計算機１とクライアント計算機５との間で共通鍵を共有するための手続きを行う。その際、クライアント計算機５からサーバ計算機１へ、公開鍵で暗号化した共通鍵のもととなるデータを送信する。サーバ計算機１は、キーサーバ３へ、公開鍵で暗号化した共通鍵のもととなるデータを渡して、復号を依頼する。キーサーバ３は、公開鍵で暗号化した共通鍵のもととなるデータを該公開鍵に対応する秘密鍵で復号して共通鍵のもととなるデータを求め、これをサーバ計算機１へ返す。サーバ計算機１は、返された共通鍵のもととなるデータをもとにして共通鍵を生成する。

【選択図】　　図１

特願２００３－０４１４８５

出　願　人　履　歴　情　報

識別番号　　［０００００３０７８］

１．変更年月日　　２００１年　７月　２日
［変更理由］　　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝

２．変更年月日　　２００３年　５月　９日
［変更理由］　　名称変更
住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝